UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,728	10/31/2001	Richard Paul Tarquini	10017270-1	3625

7590 04/07/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/001,728
Filing Date: October 31, 2001
Appellant(s): TARQUINI ET AL.

James L. Baudino
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 26, 2006, appealing from the Office action mailed September 22,2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct, except for claim 2. A Correct statement of the status of the claims follows below:

The Examiner would like to note that although on page 12 of the office action dated September 22, 2005, it was indicated that claim 2 was rejected as being unpatentable over **Kouznetsov** (U.S. Patent No 6,725,377B1) **in view Holland** (U.S. Patent No 6,851,061),Appellant on page 3 of his appeal brief under the title, **"Grounds of Rejection To Be Reviewed on Appeal"**, wrongly presented claim 2 as if it was rejected as being unpatentable over **Holland** (U.S. Patent No 6,851,061) in view of **Smaha** (U.S. Patent No. 5,557,742).

Therefore, a Correct statement of the status of the claims follows below:

- **Claims 1 and 3-10** stand rejected under 35 U.S.C. 102 as being anticipated **Kouznetsov** (U.S. Patent No 6,725,377B1)
- **Claims 2** stands rejected under 35 U.S.C. 103 as being unpatentable over **Victor Kouznetsov** (U.S. Patent No 6,725,377B1) **in view of Holland** (U.S. Patent No 6,851,061) and
- **Claims 11-13** stand rejected under 35 U.S.C. 103 as being unpatentable over **Holland** (U.S. Patent No 6,851,061) in view of **Smaha** (U.S. Patent No. 5,557,742).

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct with respect to **claims 1 and 3-13**, however is **incorrect** with respect to **claim 2**. Appellant wrongly presented claim 2 as if it was rejected as being unpatentable over **Holland** (U.S. Patent No 6,851,061) in view of **Smaha** (U.S. Patent No. 5,557,742), nevertheless, Examiner asserts that on page 12 of the final office action dated September 22, 2005, it was indicated that claim 2 was rejected as being unpatentable over **Kouznetsov** (U.S. Patent No 6,725,377B1) **in view Holland** (U.S. Patent No 6,851,061).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,725,377	Kouznetsov	04-2004
6,851,061	Holland	02-2005
5,557,742	Smaha	09-1996

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. **Claims 1 and 3-10** are rejected under 35 U.S.C. 102(e) as being anticipated by **Victor Kouznetsov** (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1)

2. **As per claim 1 and 9-10, Kouznetsov** a mobile device operable in a mobile telecommunications network, comprising:

   - **A memory module for storing data in machine readable format for retrieval and execution by a central processing unit**; [Column 1, lines 53-55;column 4, lines 43-47; column 4, lines 63-65; column 6, lines 58-61; column 10, lines 19-22] (The anti-intrusion software program which is stored on the CD-ROM or floppy disk, is installed on any computer/server by the system administrator as explained on column 4, lines 43-47 and column 4, lines 53-55 and the system administrator is required to retrieve and install the latest versions of the

updated anti-intrusion program on each servers/computers. Therefore, inherently, this program is installed in the computers memory and any computer larger or small, must have a central processing unit for execution of this software program installed in its memory module.)

- **An operating system operable to execute an intrusion detection application stored in the memory module.**[Column 6, lines 32-34;column 7, lines 46-48;column 2, lines 39-41] (First as explained on column 2, lines 25-26 and column 2, lines 32-35 it has been disclosed that the **CyberCop Network** which is the real time intrusion detection application software is offered in a variety of outlets and forms. It is accompanied by documentation including the **CyberCop Network** for windows NT version 2 **operating system**. The anti-intrusion monitor server which has stored the intrusion application software manually by the administrator in its own memory module as explained on column 4, lines 43-47, performs program execution using Pentium based server running Window NT operating system as explained on column 6, lines 32-34].

3. **As per claim 3, Kouznetsov** discloses the device as applied to claim 1 above. Furthermore **Kouznetsov** discloses the device wherein the intrusion detection application further comprises an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file and pass the signature file to the associative process engine, the associative process engine operable to analyze a data packet with the signature file. [Figure 2, column 7, lines 31-38] (The intrusion application which is first loaded at central anti-intrusion server shown at figure 5, ref. Num "514" transmits the modified attack/pattern or signature file to the push administration and the push administration transmit the modified

attack/pattern or signature to the anti-intrusion server shown on figure 2, ref. Num "202" meets the recitation of the claim.)

4. **As per claim 4, Kouznetsov** discloses the device as applied to claim 1 above. Furthermore **Kouznetsov** discloses the device further comprising a storage media, the storage media operable to maintain a database of a plurality of signature files therein.[column 7, lines 62-67]

5. **As per claims 5-8, Kouznetsov** discloses the device as applied to claims above. Furthermore **Kouznetsov** discloses the device wherein the intrusion detection application identifies a correspondence between the signature file and a data packet, a determination that the data packet is intrusion-related made upon identification of the correspondence. [Column 7, lines 31-38]

Claim Rejections - 35 USC § 103

6. **Claims 11-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061) in view of **Smaha et al**, (hereinafter referred to as **Smaha)** (U.S. Patent No. 5,557,742)

7. As per claims 11-13, Holland discloses a node [figure 1, ref. Num "11"' ref. Num "12"] of a network for managing an intrusion detection system,[Column 1, lines 15-18; figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] (The present invention relates in general to network intrusion detection data collection and, in particular, to a system and method for intrusion detection data collection using a network protocol stack multiplexor). The node comprising:

- **A memory module for storing data in machine readable format for retrieval and execution by the central processing unit**; [Column 4, lines 23-29]

- **An operating system** [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers) and

- **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and

operable to execute an intrusion protection system [Column 4, Lines 52-53;figure 2, ref. Num "37" and column 4, lines 31-32]

Holland does not explicitly disclose

- Management application, the management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link.

However, in the same field of endeavor, **Smaha** discloses

An application operable to receive text-file input defining a network-exploit [figure 1, ref. Num "20" and "12"; figure 5a, ref.Num "12"; column 4, lines 40-49] (For instance, input mechanism shown on figure 1, ref. Num "20" receives input from any wide array of sources for example user devices shown on figure 1, ref. Num "22") and **convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, [figure 5a, ref. Num "144"; column 5, lines 10-12; Column 6, lines 9-11]** (The misuse engine shown on figure 1, ref. Num "30" converts the input into events/signature and compare it with the known signatures and generate a signature representative of an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32"**)** and **the node operable to transmit the signature file to a radio frequency link**.[column 6, lines 15-17; figure 1, ref. Num "36" and "38" and ref. Num "40"] (the output signal is sent to the communication links.)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of converting the input into events/signature and compare it with the known signatures and generate a signature representative of

an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32" and transmitting to the communication links as per teachings of Smaha in to the method of analyzing the traffic using signature-based and statistical-based intrusion detection techniques as taught by Holland, in order to create a system a system capable of automatically recognizing intrustions and misuses.(See Smaha, Column 3, lines 9-10)

8. **Claims 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Victor Kouznetsov** (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1) **in view of Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061)

9. **As per claim 2**, **Kouznetsov** discloses a device or a method of monitoring intrusion using an anti-intrusion monitor server running Window NT operating system. [Column 6, lines 32-34]

Kouznetsov does not explicitly discloses

- The operating system further comprises a network stack comprising a protocol driver, a media access control driver, the intrusion detection application comprising an intermediate driver bound to the protocol driver and the media access control driver.

However, in the same field of endeavor, **Holland** discloses

An operating system [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers)

- **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and

- **The intrusion detection system implemented as an intermediate driver [Figure 2, ref. Num "37"] and bound to the protocol driver** [figure 2, ref. Num "33"] and **the media access control driver**.[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as an intermediate driver and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because

the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the operating system as per teachings of **Kouznetsov** in to the method of operating system which comprises the network stack as taught by **Holland**, in order to relates network intrusion detection with respect to a network protocol stack.

(10) Response to Argument

Referring to the independent claim 1, Appellant wrote the following in support of his argument, "The reference on the record, namely **Kouznetsov** does not disclose or even suggest "an intrusion detection application stored in the memory module" of a "mobile device operable in a mobile telecommunications network" as recited by independent Claim 1, nor has the Examiner explicitly identified any such disclosure in Kousznetsov. Thus, for at least this reason, Kouznetsov does not anticipate independent Claim 1."

Examiner disagrees with this argument,

First of all, what is argued by the appellant is the limitation which is part of preamble but was not part of the body of the claim 1.

An intended use clause found in the preamble is not afforded the effect of a distinguishing limitation unless the body of the claim sets forth structure which refers

back to, is defined by, or otherwise draws life and breath from the preamble. See In re Casey, 152 USPQ 235 (CCPA 1967).

Referring to this independent claim 1 the limitation, "A mobile device operable in a mobile telecommunications network" is the preamble part and the rest of the following limitation recited as, " A memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

An operating system operable to execute an intrusion detection application stored in the memory module" is the body part of the claim.

It is undoubtedly clear the body of this claim indicated above, neither set forth structure which refers back to the preamble, nor defined by/from the preamble.

Besides, the body of the claim does not draw life and breath from the preamble.

Furthermore, all the limitation of the body of the independent claim 1 is disclosed by the reference on the record (**Kouznetsov**). (Refer to claim 1).

Only dependent claims 7, 8 and 9 incorporate "the mobile device" in the body of claim.

However, Examiner would point out that, **Kouznetsov on column 1, lines 55-59, discloses the following.** "By server, what is meant is **any type of computer on which the software program is loaded**. This server, hereinafter referred to as an "anti-intrusion monitor server," examines packets that pass on the network and looks for characteristics of known attacks." Examiner further points out that **any type of computer on which the software program is loaded** meets the limitation of portable device.

Therefore, appellant argument regarding claim 1 and claim 3-10 that depend therefrom is not persuasive and rejection remains valid.

Referring to claim 2, rejection, appellant incorrectly stated the ground of rejection.

Appellant wrongly presented claim 2 as if it was rejected as being unpatentable over **Holland** (U.S. Patent No 6,851,061) in view of **Smaha** (U.S. Patent No. 5,557,742), nevertheless, Examiner asserts that on page 12 of the final office action dated September 22, 2005, it was indicated that claim 2 was actually rejected as being unpatentable over **Kouznetsov** (U.S. Patent No 6,725,377B1) **in view Holland** (U.S. Patent No 6,851,061).

Appellant presented argument referring to claim 2 is not based on the actual grounds of rejection and therefore not persuasive. However examiner would also point out that the all limitation of this claim is disclosed by the combination of the references namely **Kouznetsov and Holland** . [Refer to claim 2]. Therefore, the rejection remains valid.

Referring to claims 11-13, Appellant argued that neither Holland nor Smaha, alone or in combination, discloses, teaches or suggests the limitations of independent claims claim 11 and therefore argued that claim 11 and claims 12 and 13 that depend therefrom, are in condition for allowance.

Appellant argument is based on the following limitation recited in claim 11:

> "Management application, the management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link."
>
> Appellant argued that the above limitation is not disclosed by the secondary reference namely Smaha. Appellant wrote the following in support of his argument.

Smaha appears to disclose that information such as log records and audit records are converted to an "event" (defined as "an instant security state of the system" at column 5, lines 7-8 of Smaha), and then Smaha compares the event to a signature. In contrast, Claim 11 recites an intrusion protection system management application . . . operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature" (emphasis added).

Accordingly, neither the portion of Smaha referred to by the Examiner nor elsewhere in Smaha appears to disclose, teach or suggest at least this limitation of Claim 11. To the contrary, in Smaha, the "convert to event" corresponding to reference numeral 144 of Smaha referred to by the Examiner is clearly not a network-exploit rule nor is the information referred to by the Examiner "converted ...into a signature file comprising machine-readable logic representative of an exploit-signature" as recited by Claim 11 .

Examiner disagrees with this argument and would point out that **Smaha** discloses

> **An application operable to receive text-file input defining a network-exploit** [figure 1, ref. Num "20" and "12"; figure 5a, ref.Num "12"; column 4, lines 40-49] (For instance, input mechanism shown on figure 1, ref. Num "20" receives input from any wide array of sources for example user devices shown on figure 1, ref. Num "22") and **convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, [figure 5a, ref. Num "144"; column 5, lines 10-12; Column 6, lines 9-11]** (The misuse engine shown on figure 1, ref. Num "30" converts the input into events/signature and compare it with the known signatures and generate a signature representative of an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32")

Smaha further discloses, " **A signature is the set of events and transition functions that define the sequence of actions that form a misuse**.[see column 5, lines 10-12]. Likewise Smaha discloses "Misuse engine 30 uses these events to determine the existence of an actual processing system misuse. Before misuse engine 30 begins processing, however, input mechanism 20 for selectable misuses permits narrowing the scope of analysis to a specified set of misuses meets the recitation that input mechanism sets a network-exploit rule. If this rule are not set, the converting process would not follow. Misuse engine 30 then begins converting process inputs 12 into events and compares the events to signatures[see column 6, lines 9-11] meets the limitation of converting the text file input into a signature file" [See column 6, lines 9-11]. The fact that the input are converted in to events is explicitly disclosed. If these events had not been equivalent to signature file, they would not have been able to be compared with signature files. (It is very clear for one of ordinary skill in the art that only the same parameters can be compared. Different parameters would not be compared, since it is meaningless to do so.)

Appellant finally argued that neither Holland nor Smaha, alone or in combination, appears to disclose, teach or suggest that the node is operable to transmit the signature file to mobile device over a radio frequency link" as recited by Claim.

Examiner disagrees with this argument and would point out that **Smaha** discloses the following on column 6, lines 9-21].

Misuse engine 30 then begins converting process inputs 12 into events and compares the events to signatures. Misuse engine 30 generates a misuse output upon detecting a misuse during processing system operation. The misuse output consists of two outputs.

One output is output signal 32 which misuse engine 30 may send through output signal mechanism 32 to one or more of storage device 34, network 36, **communications link 38 and computer memory device 40 meets the limitation of transmitting signature file to the mobile device over a radio frequency link**. The other possible output from misuse engine 30 goes to output report mechanism 38. Output report mechanism 38 may send output reports to one or more of storage device 44, **communications link 46, network 48, meets the limitation transmitting signature file to the mobile device over a radio frequency link.**

For detailed explanation how each limitation of the claim is disclosed by the combination of references namely Holland and Smaha, refer to the claim rejection recited above.

Referring to claim 11, It has been observed that Appellant argument generally attacks references individually in a 103 rejection. Examiner would points out that Appellant cannot show non-obviousness by attacking references individually where, as here the rejection is based on the combination of references namely Holland and Smaha. (In re Keller, 208 USPQ 871 (CCPA 1981)).

Appellant last argument is regarding the dependent claims 12 and 13, that are depending on to the respective independent claim 11.

Appellant argued that since the independent claim 11 is allowable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claim.

In response to the above argument by the Appellant, the examiner replies that the respective dependent claims 12 and 13 stands or fall with the independent claim 11.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Samson Lemma
S. L.
03/23/2006

Conferees:

Kim Vu

Chris Revak

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100